

# ARMY COMMUNICATOR

## *Multi-Domain Effects*

### **Plus:**

- *DoD Network Defenders*
- *Generational Perspectives*
- *Signal History*



# Contents

## 3. Leadership

## 4. High Value Targets

## 6. Multi Domain Task Force

## 8. Mission Command Concept

## 10. Cloud Formations

## 13. Generational Perspectives

## 14. Signal History

## 16. Army-wide Focus

The Army Communicator is published as a command information e-publication for the men and women of the United States Army Signal Corps under the provisions of AR 360-1. Opinions expressed herein do not necessarily reflect the views of Office, Chief of Signal, the US Army or the Department of Defense.

Submit articles, photos, graphics, videos, story ideas, and nominations for “Signal Spotlight” to the editor [here](#). For additional information, please call (706) 791-7325.

Follow the Signal Regiment on Facebook [here](#).

Follow the Signal School Commandant on Twitter [here](#).

Col. James D. Turinetti IV  
U.S. Army Signal School Commandant

Command Sgt. Maj. Darien D. Lawshea  
Signal Corps Regimental Command Sergeant Major

Chief Warrant Officer 5 Chris R. Westbrook  
Signal Corps Regimental Chief Warrant Officer

Laura Levering  
Editor

### **On the Cover**

*Soldiers assigned to 1st Battalion, 6th Field Artillery Regiment, 41st Field Artillery Brigade fire M31 Guided Multiple Launch Rocket Systems from their M270A1 MLRS during the Thunder Cloud live-fire exercise in Andoya, Norway on the night of Sept. 15, 2021. Thunder Cloud was designed to test out the targeting capability of the High Altitude Balloon system coordinated through the 2nd Multi-domain Task Force-Europe using long-range precision fires on a seaborne target 20 kilometers off the coast on Andoya, above the Arctic Circle. (Photo by Maj. Joe Bush)*

## Team Signal,

Welcome to another edition of the Army Communicator.

The Regimental Command team visited Fort Knox, Kentucky, to meet with several organizations and tenant units across the installation including U.S. Army Human Resources Command (HRC), U.S. Army Cadet Command (USACC), and U.S. Army Recruiting Command (USAREC) to address manning and recruiting in the Regiment. The trip was centered on the bi-annual HRC Career Management Field (CMF) Review to the leadership of the Office Chief of Signal. The review focused on the branch's areas of concentration (AOC) and military occupation specialties (MOS) strength and posture, talent management, promotion analysis, and addressed future initiatives and challenges facing the branch. During the visit to USAREC, the team had a conversation on methods, processes, and challenges in recruiting for the Signal Corps and the Army as a whole. A primary topic of discussion was how the Regimental team can make an impact via hometown and home station recruiting and messaging. The team also met with USACC to discuss branching, trends, and goals in how we attract and select talent for the Signal Corps across the sources of commission. Please tell your story. We are all recruiters!

U.S. Army Training and Doctrine Command's Pamphlet 525-3-1 describes multi-domain operations as operations conducted across multiple domains and contested spaces. This month, we examine the Army's expanded focus on solutions to solve the problem of layered standoff in a multi-domain environment – specifically, where we belong and what our roles are in this space.

We appreciate all that you do and continue to do for our Army and the Nation.

*Pro Patria Vigilans!*



**Col. James Turinetti IV**  
**Signal School Commandant**



**Command Sgt. Maj. Darien Lawshea**  
**Regimental CSM**



**Chief Warrant Officer 5 Chris Westbrook**  
**Regimental CWO**



# High Value Targets

## *DoD Network Defenders identify threats*

*Col. Mark D. Miles*  
*7th Signal Command*

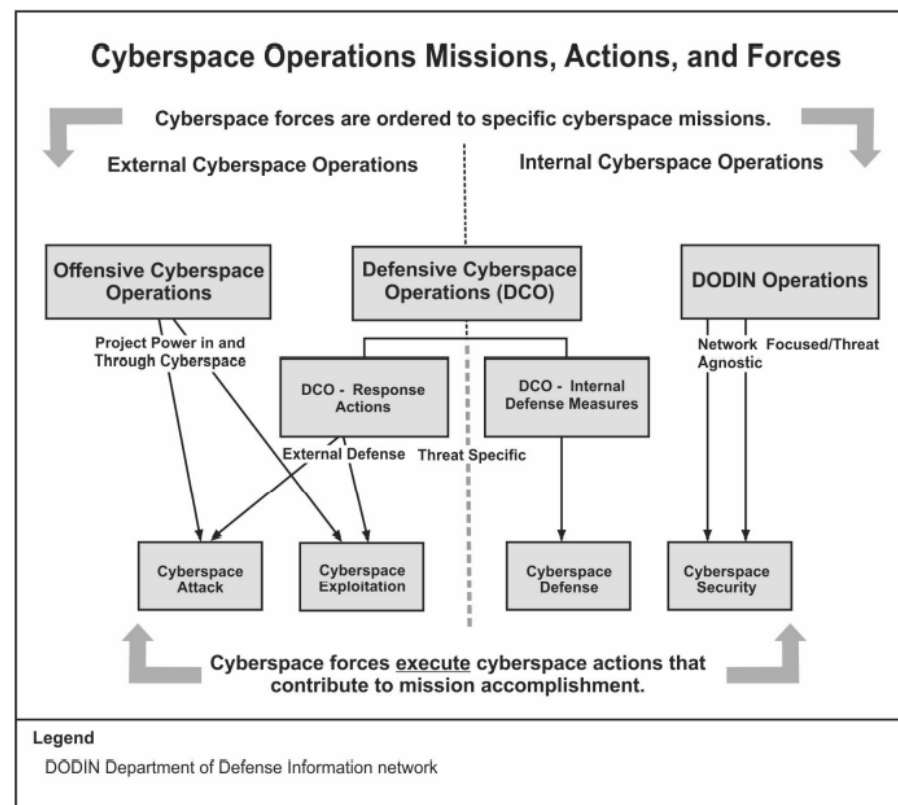
In early 2020, the Joint Force Headquarters – Department of Defense Information Network (JFHQ-DoDIN) identified a vulnerability in Virtual Private Network (VPN) hardware at key locations across the DoD network, and intelligence indicated our adversaries had the means to exploit it. VPNs are high-value targets because they allow trusted connections into our networks. Within 14 days, we patched all open vulnerabilities, put sensors in place to alert us to future adversary attempts against our network and moved on to the next priority threat.

A few days later, a network administrator noticed some unauthorized activity indicating an adversary had leveraged the VPN vulnerability before we patched it. We immediately employed our specialized cyber defensive forces, who then spent the next month clearing the infected portions of the network, at a high cost to resources and productivity.

I generalized some of the key details above, but this true story exemplifies how, as DoD network defenders, we move sequentially from identifying a threat, securing the network, monitoring the network, then engaging defensive forces (when required). While we improved all of these capabilities in recent years, threat actors around us have only gotten faster, and the threats they pose more complex. To keep pace, the Army must relook the relationship between those who conduct what we define today as “DoDIN Operations” and “Defensive Cyber Operations (DCO).”

Moreover, AR 3-12 defines DoDIN Operations as “securing, configuring, operating, extending, maintaining and sustaining” the DoDIN, and defines DCO as being responsible for “defending” the network.

Today, we mostly employ cyber defensive forces as a reaction to a failed security operation that was discovered during network



**Figure 2-2. Cyberspace operations missions and actions**

Figure 2-2 of Army Regulation 3-12 (page 2-6) is a visual representation of current Army doctrine. The chart differentiates threat-specific vs threat-agnostic operations, and shows cyberspace security and cyberspace defense as two discrete functions. As a result, different Cyberspace Forces separately track and manage the elements that identify threats, implement cyber security, monitor network status, and employ specialized defensive forces.

monitoring. To respond quicker to, or prevent, adversary infiltration we must integrate DoDIN Operations and DCO. This integration would enable: - a commander to engage with his cyber defense counterparts as soon as they identify a threat; and

- cyber security and cyber defense to reinforce each other and inform each other in real time; soon as they identify a threat; and
- cyber defensive efforts to begin earlier, and be targeted to the most critical—or most vulnerable—areas based on current network status.

This approach enables a more informed view of the threats we face and the status of our network security, which supports rapid decision-making involving a range of resources and tools. In essence, it moves Army Information Operations away from a largely reactive cyber security posture, toward one of more proactive protection.

How can we achieve this paradigm shift? First, we start with a focus on education at all operational levels to ensure “security,” “operations,” “intel,” and “defense” elements speak the same language. Specialists and leaders in all of those areas must have the same basic understanding of the systems employed on the network and what resources exist to support those systems. Every echelon with a NETOPS section needs an expanded and more informed view of the networks under their purview, and leaders at every echelon must be more aware of what threats exist, or could exist, against their key networked capabilities—and where they may be accepting risk today.

We must also add structural linkages between NETOPS and cyber defensive organizations and personnel. This could take the shape of liaison positions or mechanisms that facilitate greater communication and closer coordination between the two functions. These linkages create and build relationships that lead to easier and faster identification of threats and vulnerabilities, leading to earlier and more informed cyber defensive efforts.

Not only will these changes improve our security posture, but they also position the Army for success in our drive to modernize and converge the network:

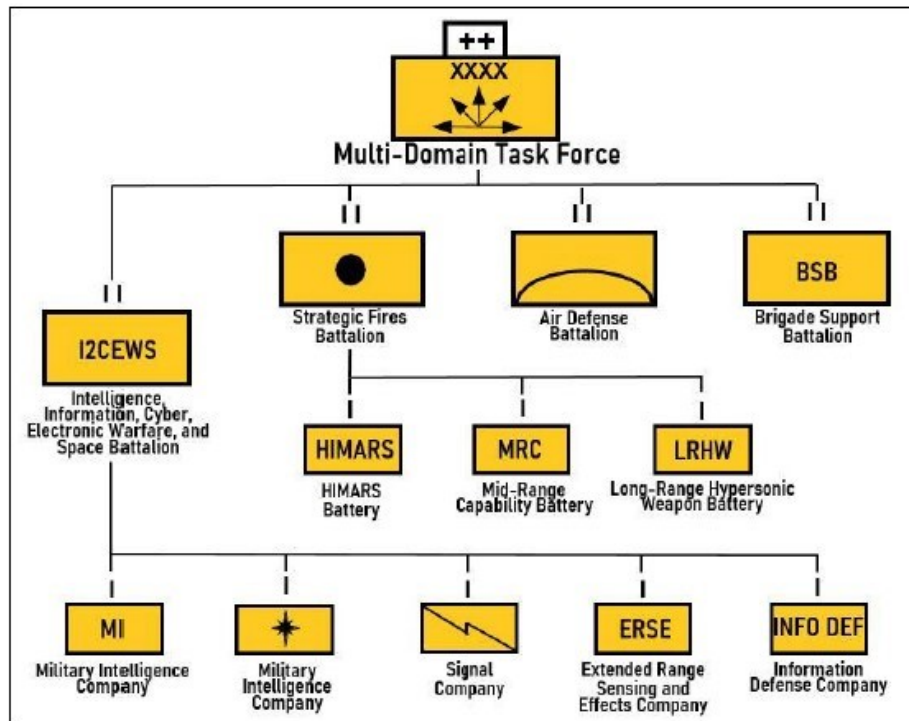
- With expanded awareness through education, we can effectively implement and employ key technology advancements such as zero trust, artificial intelligence, machine learning, cloud migration, and many others.
- The linkages we put in place will facilitate better planning, smoother rollouts, and easier post-implementation evaluation and analysis.

In the near future, the Unified Network will link previously segmented security boundaries—making the DoDIN-A a bigger and potentially more vulnerable target. Commanders must be able to maneuver forces, conduct security operations, and adjust to threats simultaneously in this environment. To do that, we must expand our basic understanding of what cyber defense is, change our view of who the cyber defenders are, and implement a cohesive and coordinated cyber defense at echelon that is nested in the greater Army system.

# Signal in the Multi-Domain Task Force

*Capt. Marissa Leibman and Rob Murray*  
*1 MDTF; RID CCoE*

**Figure 1. Notional Generic MDTF**



**Source:** Chief of Staff Paper #1 Army Multi-Domain Transformation Ready to Win in Competition and Conflict, March 16, 2021, p. 12.

The Army's Multi-Domain Task Forces were formed in response to the threats posed by a resurgent Russia and China. The Army assessed that it required units capable of operating in a multi-domain (air, land, water, space, cyber, information) environment. The MDTF is designed to operate as a Theater-level maneuver element that provides precision fires and effects in all domains in support of the joint force. The



*U.S. Army Soldiers look at a screen for electronic warfare (EW) training during Combined Resolve XV, Feb. 23, 2021 at the Hohenfels Training Area. Combined Resolve XV is a Headquarters Department of the Army directed Multinational exercise. EW is a key enabler within the MDTF. (Photo by Sgt. Julian Padua)*

MDTFs are designed to serve as the cutting edge of innovation for the conventional Army.

The Multi Domain Effects Battalion (MDEB), formerly known as the Intelligence, Information, Cyber, Electronic Warfare, Space, and Signal (I2CEWS) Battalion, is designed to provide space, cyber, and information effects, as well as conducting operations in the electromagnetic spectrum (EMS). As a Signaleer, you will support high data throughput for information dominance operations, intelligence, cyber, electronic warfare, and space missions. The MDEB fields and tests some of the Army's newest equipment and your work on these systems will be reported directly to Army Futures Command.





*Newly activated U.S. Army 2nd Multi-Domain Task Force and 41st Field Artillery Brigade test sensor to shooter capabilities during “Thunder Cloud.” (Photo by Spc. Joshua Thorne)*

Your work will also impact the equipment the rest of the Army is fielded and will be vital to ensure the Army is able to compete and win against our adversaries.

Signal officers (25A) serve on the cutting edge of the action, as the Army pursues strategic objectives to compete and win in counter-coercion, unconventional warfare, and information warfare. Your actions will have real world impacts as the Army seeks to deter escalation as well as to set conditions for an expeditious transition to armed conflict if needed. As a 25B, 25Q, or 25S you will travel as part of a highly deployable network extension node team. The primary equipment of the MDTF is fielded on the ESB-E framework. Standard equipment you will work with include the Scalable Network Node (SNN) with Hawkeye and Phoenix-E terminals, Transportable Tactical Command Communications (T2C2) Lite and Heavy, GRRIPS (Global Rapid Response Information Package), MuOS (Mobile User Objective System), TACSAT, and JBCP. Additionally, you will learn how to field-craft HF antennas by hand. Recently, we have even tested several low earth orbit, direction finding, and AI-based systems that you will weave into your network. This is a job for people with a strong sense of initiative, creativity, and the drive to achieve mission success, and the integrity to voice when a system is not meeting the standards required.

*Do you have what it takes to become part of the Multi-Domain Effects Battalion?*



*Soldiers assigned to 1st Battalion, 6th Field Artillery Regiment, 41st Field Artillery Brigade fire M31 Guided Multiple Launch Rocket Systems from their M270A1 MLRS during the Thunder Cloud live-fire exercise in Andoya, Norway on the night of Sept. 15, 2021. Thunder Cloud was designed to test out the targeting capability of the High Altitude Balloon system coordinated through the 2nd Multi-domain Task Force-Europe using long-range precision fires on a seaborne target 20 Kilometers off the coast on Andoya, above the Arctic Circle. (Photo by Maj. Joe Bush)*

# I Corps tests distributed mission command concept in Indo-Pacific

## Communications networks prove critical

**Dr. Raj Iver**  
*U.S. Army Chief Information Officer*

Challenged to think and act differently in the Indo-Pacific region, America's First Corps tested a concept that suggests the traditional Corps structure might not be relevant while operating in a region that's predominantly maritime.

Given the opportunity to experiment, the Corps headquarters partnered with the U.S. Air Force and U.S. Navy to exercise a first-of-its-kind distributed mission command concept west of the International Date Line.

"We've got to be present in the Pacific," said I Corps Chief of Staff Brig. Gen. Patrick Ellis, "In order to do that, we need to be scalable, because scalability enables us to be more agile, resilient and survivable. So, to operate in the doctrinal way that Corps are built doesn't necessarily make the most sense to us. We're taking it apart and rebuilding it in a way that enables us."

First Corps' operational reevaluation involves creating a nodal mission command construct, experimenting with multiple smaller nodes in different locations.

"We're going to be collective, connected, but not co-located," said Ellis. "We think dispersal is the key out here in the Pacific. This way, we're able to move around faster, and we're not as big as a target, potentially, for any adversary."

To test this theory, a four-Stryker vehicle package with roughly 20 personnel and a robust communications capability flew via two C-17 Globemaster III aircraft from Joint Base Lewis-McChord, Washington, to Andersen Air Force Base, Guam. After performing mission command activities in flight, the small Corps node embarked aboard the United States Naval Ship City of Bismarck to prove an unprecedented Army Corps capability — executing mission command afloat.

"Establishing a communications network baseline that is inherently joint is critical," said Col. Elizabeth Casely, I Corps Communications (G6) Director. "Service-agnostic, sensor to shooter, flat architecture; once we've established that common network, we can pop in or pop out with all of our capabilities and exchange that information freely."



*Soldiers assigned to America's First Corps and Airmen assigned to Joint Communications Support Element set up and perform communication checks aboard the USNS City of Bismarck at Naval Base Guam, Feb. 16, 2022. Partnered with the Joint Force, I Corps is conducting a training operation in Guam that enhances readiness, showcases joint interoperability and exercises distributed mission command in the Pacific.*

*(Photo by Spc. Jailene Bautista, 5th Mobile Public Affairs Detachment)*

Casely's small team of signal support specialists from I Corps, augmented by the Joint Communications Support Element, MacDill Air Force Base, did just that, and capitalized on the opportunity to explore distributed mission command possibilities in a nautical environment. "We integrated Army mission command systems with Navy network, traversing Navy satellite communications, which landed at a Joint teleport, then split off to an Army point of presence and then routed back into a larger joint network," explained Casely. "We've Lego-bricked all of this together allowing us to validate a proof of concept that is joint integrated command and control."





*I CORPS est Comms U.S. Army Soldiers assigned to America's First Corps establish communications aboard the USNS City of Bismarck at Naval Base Guam, Feb. 22, 2022. Partnered with the Joint Force, I Corps is conducting a training operation in Guam that enhances readiness, showcases joint interoperability and exercises distributed mission command in the Pacific. (Photo by Spc. Preston Robinson)*

"We really want to become transport-agnostic," agreed Ellis. "We don't want to be emotionally attached to how we're moving data, we just need to be able to move it."

Leveraging their technological capabilities, the Corps also experimented with moving data via cloud computing.

"If we can tap into a persistent information environment that is supported by cloud computing, that makes things a lot easier," said Casely. "You're changing your setup times now from weeks or days to potentially a couple days or hours. Today, we're in the very nascent stages of determining how cloud computing optimizes distributed C2, but I'm confident about where we're headed."

While much of the Corps' experimentation of the nodal construct was technologically centric, Ellis said reassessing how the Corps operates involves the entire staff.



*U.S. Army Sgt. Jimmy Nguyen, a signal support systems specialist with America's First Corps, left, and Sgt. Jeremy Braden, a satellite communication systems operator-maintainer with Joint Communications Support Element, establish communications onboard the USNS City of Bismarck at Naval Base Guam, Feb. 9, 2022. Members of America's First Corps deployed from Joint Base Lewis-McChord to Guam to conduct a training exercise that enhances readiness, showcases joint interoperability and exercises distributed mission command in the Pacific. (Photo by Spc. Richard Carlisi)*

"This isn't just a communications challenge," said Ellis. "We see this as a 'whole-of-staff' challenge. The hardest part out of all of this isn't the technological aspect, it's the process. It's taking us out of our comfort zone with respect to operating in large single locations. It's causing us to rethink how we do business, and really, it's about figuring this out as a team."

Casely said that being on a team in a dynamic, learning organization is transformative and contributes to continued success.

"We basically tested a hypothesis, and produced tangible results," she said. "It's not theoretical anymore. It is no longer academic. So the question is, what's next? The possibilities for the Corps are endless."

# CLOUD FORMATIONS

*The Army lays the foundation for data-centric operations.*

*Lt. Col. Philip J. Smith, Paul Puckett III and Col. Evert R. Hawk II*

Shoot, move and communicate. All three fundamentally involve movement. It can be moving a small chunk of lead to its intended target or moving raw materials to ammunition plants. It can be placing Soldiers in the right situation with the right mission to move to a specific objective. It can be moving information in the form of data from the location of observation to an analysis center, then back to field commanders for decision-making at the pace of war. But the real challenge is delivering payloads to their intended targets simultaneously in a constantly moving and therefore changing environment.

In each of the examples above, we find that access to real-time information is critical to ensure that we are shooting, moving and communicating the right way. As DoD pointed out in its 2020 DoD Data Strategy, and the U.S. Army has pointed out in the Army Data Plan and Joint All Domain Command and Control (JADC2) documents, data has become the new ammunition in a changing battlefield. Similar to moving ammunition, we must be able to move relevant data to the right users in time to make a difference. The U.S. Army Network Cross-Functional Team, part of Army Futures Command, is enabling the Army to leverage modern concepts and technologies to access and evaluate data from numerous sources, enabling faster and better informed decisions.

The foundational concept on which many other concepts and technologies will be built is the cloud: the ability to remotely access data and services via an internet connection. In the same way we build physical structures, this foundation—while not as visible to the unknowing eye—is critical to a stable end-state complete with a frame, walls, plumbing and electrical. In this multi-part series, we aim to describe the Army's tactical cloud progress to date, as well as challenges to consider moving forward. We also explain key cloud terms where common understanding will be mandatory within the requirements, communications, acquisition, tactical and general leadership communities. The foundational concept on which many other concepts and technologies will be built is the cloud: the ability to remotely access data and services via an internet connection. In the same way we build physical structures, this foundation—while not as visible to the unknowing eye—is critical to a stable end-state complete with a frame, walls,



*The 50th Expeditionary Signal Battalion (Enhanced) and 63rd Expeditionary Signal Battalion conducted a combined large-scale combat operations communications exercise at Fort Bragg, North Carolina, on Sept. 29, 2021. Operational units are experimenting with hybrid tactical cloud models that provide access to critical services in disadvantaged or contested environments and additional resources when network connection allows.*

*(Photo by Capt. Eric Messmer)*

moving forward. We also explain key cloud terms where common understanding will be mandatory within the requirements, communications, acquisition, tactical and general leadership communities.

## WHAT THE CLOUD BRINGS TO DoD

Often “cloud” takes on two very different but complementary meanings. One approach focuses on the value of access to data in the cloud—think backing up the photos on your smartphone—while the



other focuses on the infrastructure that enables that access. The second version, often referred to as cloud computing, means that computing and storage capabilities require hardware and therefore, must exist somewhere. That can be your pocket, in the form of a smartphone, or your laptop or Internet-of-Things-like device. It can be warehouses full of high-end servers and networking equipment. For larger workloads (such as artificial intelligence, data analysis, service hosting), it requires specialized hardware purposefully built to handle the kind of computing needed to create complex machine-driven neural networks. It can also include the small collection of servers and networking kits Soldiers take to the field today, or any hardware combination thereof. For DoD, acquiring and maintaining this hardware is a challenge because the uncertain nature and scale of conflict make it difficult to target investments, not only in acquisition but also in people. Cloud has become a way to offload expertise requirements and hardware investments while allowing for instant flexibility—if you need more computing and storage resources, you pay for them, click a button and they are instantly available. When they are no longer needed, you simply delete the resources you used and can reduce your cost rather than sinking an unused investment and obligation in equipment and people. However, for the tactical and operational Army, access to online cloud computing resources means bringing cloud computing resources into the field—or drastically increased reliance on the expeditionary network systems, often with bandwidth restrictions, that reach back to centralized cloud locations. Doing this in a way that meets today's mission needs and the unknown needs of the future is a major concern.

The vision most have of the cloud is that it's just someone else's computer or data center somewhere that cannot be touched or controlled. This is one of numerous models when it comes to cloud computing, called off-premise public cloud, which intends to serve numerous tenants with common cloud computing requirements. There are other models for cloud computing that start to combine both public and private cloud offerings that can be delivered in both off- and on-premise architectures. Designers and engineers can structure those different cloud environments to function as one hybrid cloud.

## **IMPLEMENTATION AND EXPERIMENTATION**

The Network Cross-Functional Team is working with the Army's Enterprise Cloud Management Agency (ECMA), Project Manager Mission Command (PM MC) and others to make this tactical hybrid capability a reality. In the beginning, the team worked with PM Mission Command on a pilot to see if current software could be served from a

## ***Understanding how the Army and DoD are approaching cloud implementation starts with defining these different cloud models.***

### ***Hyper-Scale and Off-Premise***

*Modern off-premise hyperscale cloud involves multiple (usually large) data centers with the ability to replicate data and load-balance access at large and robust scales. When you become a tenant of one of these cloud providers, you are renting a set of components of that infrastructure for use, just like renting an apartment. Depending on the agreement and cost, where and how mission-critical data is replicated and load-balanced can vary. Most cloud providers replicate data between zones within a geographically similar region—enabling load balancing and resilience of service—but can be expanded to multi-region to guard against catastrophic failure such as an earthquake, flood or malicious attack that could compromise geographic power or network connectivity.*

### ***On-Premise Cloud***

*When it comes to on-premise cloud computing serving DOD needs specifically, the community has been practicing this in select IT spaces for some time now. On-premise means services are physically in the organization's owned facilities. This could be on organization-owned equipment or equipment provided by a second or third party, such as Amazon's Snowball line or Microsoft's Azure Stacks. The burden of power, space, cooling and external connectivity are the minimum responsibilities of the hosting organization. Other responsibilities vary based on what services and agreements are procured with a service provider. This model provides the most autonomy for an organization but comes at the cost of dynamic flexibility.*

### ***Hybrid***

*As the world becomes more connected, industry is reevaluating how to design its systems to take full advantage of the value of cloud computing. For sectors like the oil and gas industry, where companies often operate within remote and challenged environments, a hybrid cloud architecture serves both local and global cloud computing needs. This model attempts to take the best of both previous models so that when you have connectivity, you have access to the resources available in hyperscale (robust, on-demand and flexible), and when your connection is disadvantaged or contested, you have critical services locally hosted with you. In the tactical space, this is the design we must strive for. There are times on the battlefield where loss of certain services could lead to unacceptable loss of situational awareness, obstructing command while other less critical services can enhance decision-making on a broad tactical to strategic scale when network connection allows.*



cloud without operating outside of current contract constraints. PM MC, the Network Cross-Functional Team and the Pennsylvania National Guard proved it was possible in a Non-classified Internet Protocol (IP) Router Network (NIPRNet) environment. Others expanded on that capability once Secret IP Router Network (SIPRNet) capabilities were available from ECMA's cArmy service, which provides an authorized and accredited set of general-purpose multivendor cloud environments that host Army IT services for multiple classifications.

Initially, PM MC, the Pennsylvania Army National Guard and the Network Cross-Functional Team collaborated on a pilot to explore the technical possibility of placing currently fielded Mission Command Information Systems, the core of the Command Post Computing Environment, in a NIPRNet cloud—because of accreditation timelines, the pilot could not expand into SIPRNet. The Tactical Cloud Pilot, Increment I validated the hypothesis that units could be trained on new software without being issued associated hardware. COVID-19 constraints forced an adaptation that also proved, while not ideal, that such training could be done remotely. Others took notice of the success and began work on their own adaptations. One U.S. Army Training and Doctrine Command use case is attempting to expand the number of users and locations, while units are striving to exercise these capabilities in tactical scenarios to inform the requirements community.

Today, we are leveraging the XVIII Airborne Corps' Project Ridgway to pilot hosting capabilities through cArmy, with Amazon Web Services in the 101st Airborne Division and Microsoft Azure in the 82nd Airborne Division. As part of Project Ridgway, which encompasses XVIII Corps data and software modernization efforts, these units are providing realistic use cases and putting them to the test with current and legacy software during various experiments and field exercises on a mix of hyperscale, commodity and vendor on-premise cloud solutions. The Network Cross-Functional Team also just began working with I Corps on upcoming events for the spring of 2022. Upon successful I Corps implementation, the Army will have initially experimented or piloted with as-is software and configuration in at least one of the two cArmy cloud options from the battalion all the way up through the corps and brigade echelons, and division in the other.

What value does this bring to the Army? These pilots demonstrate possibility. While not the ideal or most fiscally efficient arrangement of software, with the episodic nature of exercises and operations, the Army can put cloud computing to use to enable a persistent, real-time mission command environment delivering those resources as a service to the total Army. When online, every unit asset could have secure access

to the same common operating picture of resources and capabilities. In a contested environment, critical data and services for maneuvering capability will remain with the units geographically. However, much work still must be done to make this a feasible option for any program of record. In general, fielding to the cloud with as-is software is currently cost prohibitive.

## CONCLUSION

There is still much work to be done, mainly with the key tool that creates, consumes and disseminates our data: software. With the availability of dynamic computing and storage paradigms enabled by cloud computing comes a new set of challenges for how we use software. The software that the tactical Army currently owns and operates was not built to be run in the agile cloud environments in which we are placing it. The way we handle, manipulate, translate, store and visualize data in its various forms is still largely tied to specific warfighting functions, limiting the ability to inform decisions more broadly.

While the current pilots will deliver new value to the Army in the form of real-time data access, reduced technical overhead and informing operational uses of cloud resources, the Army's software was never designed to run in the cloud in optimized ways. Therefore, while the Army will see isolated value in using the cloud, software and system modernization remains fiscally unachievable at the scale the Army requires. The Army cannot change operational software across the force overnight, causing a legacy compatibility requirement as it adapts to future capabilities.

All these considerations lead to follow-on topics of the technical knowledge and strategic investment in software redesigning and re-platforming to take full advantage of cloud computing. These new means of implementing IT services may cause us to reevaluate the ways in which we employ them. Concepts of operation for how identity services are implemented and compartmented are at the root of many if not all other IT services in a secure environment, and must be addressed and resolved. While each concept brings its own advantages, the revolutionary contribution to the fight can only be delivered in its integration with the others.

# My experience joining the U.S Army

## Perspective at the Initial Entry Level

*Pfc. Amando Mendez  
Charlie Company, 551st Signal Battalion*

I joined the United States Army at age 18 and straight from high school, like many for various reasons like college tuition, financial independence, personal goals, family traditions, etc. Coming from a place where English is a second language made joining slightly challenging. Despite that, I quickly realized this is and will be one of the best decisions of my life.

Basic Training was an amazing experience. It is a learning environment which demonstrated how professional the Army is. Drill sergeants instructed us on SHARP and EO programs and how important they are to maintaining a climate free of behaviors that degrade mission readiness and undermine teamwork.

In Basic Training, we learned warrior tasks. These individual skills ensure all Soldiers must be able to do to shoot, move and communicate on the battlefield. These skills are critical to soldier survival. They include basics such as firing your weapon, reacting to contact, land navigation, first aid, and communicating on a radio. Additionally, one of the most important things is customs and courtesies, rendering honors, and preserving tradition. Additionally, drill and ceremony helped develop attention to details and working as a team.

Upon arrival to Advanced Individual Training (AIT), I started learning all the opportunities available to be successful in my career. Some examples are attending RASP (Ranger Assessment Selection Program) to join the 75th Ranger Regiment, pursuit of being a distinguished honor graduate, and taking courses on the Army United States Army Skillsoft website, in which five hours of education is equal to one promotion point. The total amount of promotion points by doing the correspondence courses is 80 points in 500 hours.

Another point that I will like to emphasize as an AIT Soldier is the creation of good habits. Creating good habits, while in AIT, is essential because they will determine your performances once you graduate and get to your first duty station. Habits like waking up early to work out are one of the best ways to start the day. You feel more energized and you have won the "morning fight," which leads to a more productive day. Also, time management is another essential skill. For me, time management helps me to optimize my free time and use it properly for productive things.

In the end, with the short time in service that I have, I believe that joining the United States Army can build up people for success by making competent individuals who live by their creed and values.

# A generational exchange

## Transitioning Army Leadership

*Spc. Brian Ray  
Charlie Company, 551st Signal Battalion*

As cliché as it may sound, there exists a difference between generations - past and newcomers to the armed services today. The socialization of our Soldiers has changed throughout the decades, especially between new Soldiers and those nearing the end of an Army career. A comparison of priorities and motives come into focus when exploring this dichotomy.

The Armed Forces, 20 to 30 years ago, was fueled by a difference society - before instant connectivity, emerging advocacy for greater emotional and behavioral health support, and protections to Soldiers with same-sex relationships. The Army may have been perceived differently than by today's incoming generation. The incoming generation's ability to interact with the outside world is greatly heightened. This greater exposure may provide distractions or differences, but does not mean the willingness to serve varies greatly.

Motivations of participants in this organization, if synchronized and emulated, can lead to overcoming resistance and motivation perspectives.

Some may liken the Army to a job comparable to those in the civilian sector, and some may not be sure of why they joined. Many current Soldiers rose to their feet and defend our homeland throughout a score of hard-fought and taxing military operations, some of which are now only coming to a close today. The service members having made this leap to a profession-in-arms share their own distinct *modus operandi*, in addition, of course, to their training experience.

One may ask where this leaves us in matching expectations of older members of the Army, their discipline, commitment to service, and success for those coming and going. While the Army has served as a conduit for career advancement for many, equally as important should be a continued and further emphasis of what it means to serve, and a renewed or revisited integration of greater soldier resiliency and pride of country in recruiting. Further, a program catering to these priority areas should make the experience more rewarding, fulfilling, and disciplined. The sacrifices and history of selfless service, and standards, or ethos, of members departed and present should be refined and magnified to build upon the core teaching of the Army's values - along with history, benchmarks for character, and exemplifications of the good worth doing.

Some may say that the new generation does not work as hard for much of what they have been given, but rather, the experience and fulfillment gap between past and present is needing rectification. Knowledge bearers of the Army must meet where future Soldiers' creative and leadership capabilities exist.

# Spencer B. Akin becomes Chief Signal Officer 75 Years Ago

## *“The best Signal Officer I have ever known”*

**Steven J. Rauch**  
*Signal Corps Branch Historian*

“I am recommending Akin’s appointment as Chief Signal Officer,” wrote Army Chief of Staff General Dwight D. Eisenhower to General Douglas MacArthur in an urgent, “eyes only” backchannel message on January 28, 1947. On the copy of the message, he provided to Brig. General Spencer B. Akin, MacArthur wrote in pencil, “To Gen. Akin. Hearty congratulations. McA.”

So who was this Akin that two of the most famous generals in U.S. military history deemed worthy of their time and confidence? It was Spencer B. Akin, who at the time was serving as Gen. MacArthur’s signal officer at Headquarters, Far Eastern Command in Tokyo, Japan as part of the post-war occupation forces. Akin had spent the entirety of WWII working for MacArthur as the Southwest Pacific Area (SWPA) theater signal officer, today known as a J6. Akin was so important to MacArthur that he was selected to be one of only 20 people, including MacArthur and his family, who evacuated via PT-boats from Bataan and Corregidor to avoid capture by the Japanese.

Spencer B. Akin was born in Greenville, Mississippi, on February 13, 1889. He graduated from the Virginia Military Institute in 1910 and was appointed a 2nd lieutenant in the infantry branch. He was initially assigned to the Philippines in 1911, and until 1917, remained in the infantry. In 1918, he began working with the Signal Corps, and as a major, he became the division signal officer of the 1st Division at Ft. Dix, New Jersey, in 1921. He later served as the division signal officer of the 1st Cavalry Division at Ft. Bliss, Texas, from 1923 to 1924. He attended the Air Corps Tactical School in 1926 and later became the assistant commandant of the Signal School at Fort Monmouth, New Jersey, from 1929 to 1932. During the 1930s, he was assigned to staff in the Office of the Chief Signal Officer, attended the Army War College, and became third Army signal officer in May 1941.

Akin was assigned to the Philippines in late 1941. He was appointed as a temporary Brigadier General on December 18, 1941, and he became the signal officer (G6) of US Army Forces, Far East. In March 1942, he accompanied MacArthur and his staff during the escape to Australia. There MacArthur established a new theater headquarters for the Southwest Pacific Area to coordinate all allied efforts to oppose further



*General Akin and his aide Capt. Starr departing Tokyo, Japan in February 1947 for the United States. Source: Spencer B. Akin Collection, Signal History Office.*

Japanese expansion, particularly the defense of Australia in 1942. He appointed Akin as the Chief Signal Officer (J6) of the theater and he would serve in that position during all of the subsequent SWPA campaigns against Japan.

On November 3, 1943, Akin was appointed as a temporary major general and in addition to his J6 duties, he commanded the theater Signal Intelligence Service and Radio Countermeasure Service, Far East. After Japan surrendered in September 1945, Akin became Chief Signal Officer for the U.S. Army Forces in the Far East on the staff of General MacArthur who served as the Supreme Commander Allied Powers in the Pacific overseeing the occupation of Japan.



For his service during the war, Akin was awarded the Distinguished Service Cross in 1942 for gallantry in action at Bataan; the Distinguished Service Medal in 1942 and 1945; the Silver Star for gallantry in 1942 and 1944; and the Air Medal for gallantry and contribution to success of the Army Air Forces in 1946.

Upon learning that a replacement was being sought for the out-going chief signal officer, Maj. Gen. Harry Ingles, General MacArthur took pen in hand, as he previously had done to secure Akin his temporary promotion to major general. On January 14, 1947, MacArthur wrote to Undersecretary of War Kenneth C. Royall asking the Army leadership to select Akin because:

“He has, during the war, been the Chief Signal Officer for All Forces (Army, Naval, and Air) under my command. . . This officer has demonstrated that he not only has the required technical knowledge, but also the administrative and executive qualifications required for appointment as Chief Signal Officer of the Army. I regard him as the best Signal Officer I have ever known.”

Interestingly, 1947 was also the year that a new national security structure would be implemented establishing the Department of Defense and separate U.S. Air Force. With that joint-force organization in mind, MacArthur added, “Akin’s experience in connection with the coordinated and cooperative integration of Army, Navy, and Air Force Signal communications render him especially well-qualified in this field at a time when unification of the Armed Forces is under consideration.”

Other generals who had benefited from Akin’s work as J6 during the war also supported him. Lt. Gen. Robert L. Eichelberger who had commanded the U.S. Army component of SWPA during the early part of the war stated: “General Akin has fought in the past five years from Bataan to Tokyo and his duties have included the great signal set-up on the continent of Australia as well as combat signal work along the chain that led from New Guinea through the Philippines. . . . Wherever I went, sooner or later General Akin would show up in the most dangerous places in order to get first-hand information for General MacArthur.”

Not only his Army colleagues but also the Air Force leadership lobbied for Akin to be selected for the job. On January 21, 1947, Lt. Gen. Ennis C. Whitehead, commander of the Far East Air Forces, wrote to the Assistant Secretary of War for Air: “I understand that a change in Chief Signal Officers is imminent. . . I hope that the next Chief Signal Officer will be one who has had extensive experience with Air Force combat units operating in the field in war . . . I have a candidate, namely, Brigadier General Spencer B. Akin. . . He is a man of great personal courage.



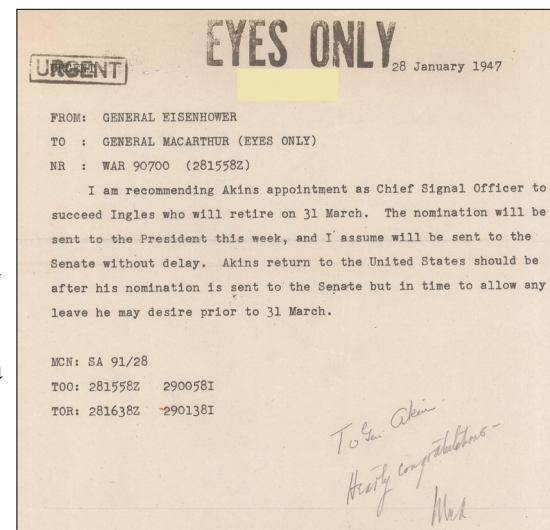
(Left) MacArthur and SWPA leaders ca. 1944. Spencer Akin is at far left; MacArthur in the middle and far right is Robert Eichelberger. Source: Spencer B. Akin Collection, Signal History Office.

(Right) Message from Gen. Eisenhower to Gen. MacArthur announcing Akin’s selection as Chief Signal Officer. Source: Spencer B. Akin Collection, Signal History Office.

I remember once in the Buna campaign when our infantry was held up at one of the causeways crossing the Buna Swamp. Everyone thought that there were many [Japanese] on the other side. Akin and one or two of his party walked across; nothing

happened, and then the infantry followed. General Akin supported me 100 percent during the entire war . . . I feel very strongly that the Air Force and the Army would profit if General Akin become the Chief Signal Officer of the Army.”

Fourteen days after the letter writing campaign began with MacArthur’s letter to the War Department, Eisenhower informed him that Akin had been approved to be the next Chief Signal Officer for the Army. During February 1947, Akin attended to turning over his responsibilities as J6 and prepared for his move back to the United States for the first time since 1941. On April 1, 1947, now-Maj. Gen. Spencer B. Akin was sworn in as the 17th Chief Signal Officer in Washington D.C. He would serve in that position until his retirement on March 31, 1951.



# April Observance:



## ‘Prevention Starts With You’

*Laura Levering  
U.S. Army Signal School*

Sexual Assault Awareness and Prevention Month (SAAPM) is an annual campaign recognized by both military and civilian communities in April. But for members of 15th Signal Brigade’s Sexual Harassment/Assault Response and Prevention (SHARP) program, the observance is constant.

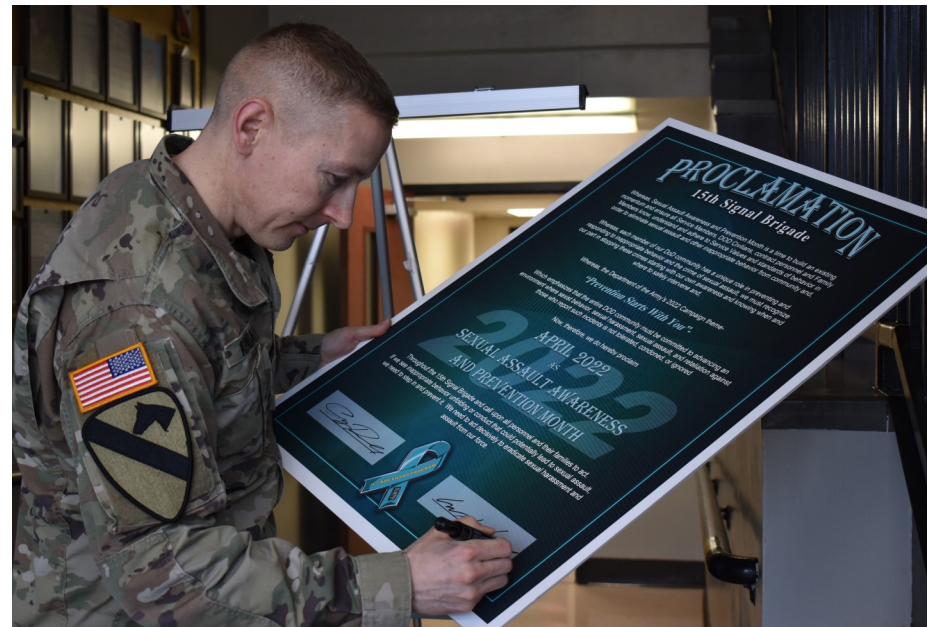
Master Sgt. Amanda Clayton, 15th Sig. Bde. sexual assault response coordinator (SARC), encourages people to view sexual assault awareness and prevention as one of their daily tasks.

“We truly want everyone to recognize and understand that this is not just a topic for April,” Clayton said. “Just as we work year-round, the focus has to be year-round as well because that is how we are going to get closer to prevention.”

This year’s theme, “Prevention Starts With You,” lines up perfectly with the message Clayton and her team want to convey through a series of events planned throughout April. Activities include weekly virtual “lunch and learns,” 5K color run, sports tournaments, and a SHARP NCO and Soldier of the Month board. Each event is designed to be educational and fun in hopes the Soldiers walk away better prepared to prevent sexual assault not only within their ranks, but also out in the community.

“The military has free training ... take advantage of it,” said Kizzy Lee, victim advocate, 15th Sig. Bde. “Use it, share and apply outside of the Army. Take what you learn to your house. You can talk to your 5-year-old, your spouse ... take it with you.”

In addition to normalizing talks about sexual assault prevention, Clayton believes that if everyone would treat each other as they would a beloved family member, it would go a long way in terms of prevention.



*Col. Edward Kendall, 15th Signal Brigade commander, kicks off Sexual Assault Awareness and Prevention Month with a proclamation signing at the Headquarters. (Photo by Laura Levering)*

“Ask yourself how you would feel if you saw a family member being treated a certain kind of way,” Clayton said. “If we value each other in the same regard, then perhaps we could get to prevention because then that dignity and respect are there. That’s how you kind of have to look at it – like your own family – because we are an Army family. And when we look at each other in that regard, then it helps us to be able to treat each other as such.”